**Internship Project Report**

# Title: Keylogger Awareness Simulator Using Python

**Intern Name:** Abinaya Balakrishnan

**Internship Period:** June 10,2025 – July 10,2025

**Domain:** Cybersecurity and Ethical Hacking

**Organization:** Tamizhan Skills

**I. Abstract**

This project simulates the operation of a global keylogger using Python for ethical awareness. The program captures every keystroke typed on the system—across any application or window—until the user presses the **ESC** key. It then presents a real-time log viewer GUI and a final awareness popup to educate users on the risks of malicious keyloggers. The goal is not to exploit, but to inform users through firsthand experience of how vulnerable they are to such attacks.

**II. Problem Statement**

Keyloggers are widely used in cybercrime to silently collect sensitive data such as passwords, personal messages, and financial details. Most users are unaware of how easily this can be done with minimal code. This project aims to bridge that knowledge gap by simulating a real keylogging scenario and raising awareness.

**III. Objective**

* To develop a working keylogger that captures keystrokes globally
* To log and store keystrokes with timestamps in a .txt file
* To display the recorded data in a GUI-based log viewer
* To show an awareness message upon stopping the logger (ESC key)
* To simulate real-world threats while maintaining ethical boundaries

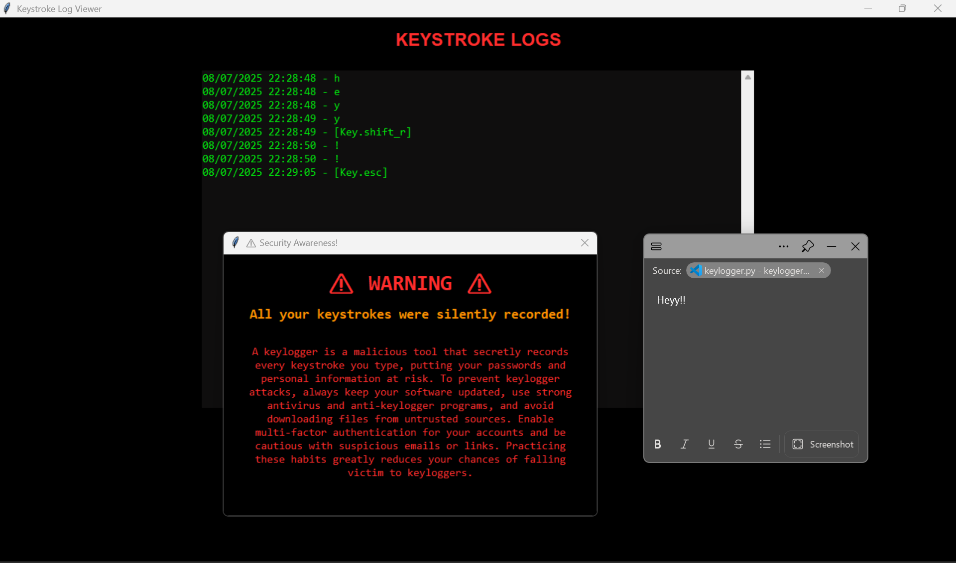
**IV. Tools & Technologies Used**

* **Python 3**
* pynput (keyboard listener)
* Tkinter (GUI viewer and awareness popup)
* ScrolledText (for displaying logs)

**V. Workflow**

1. User runs the Python script.
2. The logger starts capturing **every key press globally**.
3. Each keystroke is timestamped and written to output1.txt.
4. Pressing **ESC** stops the logger.
5. A GUI window pops up displaying the full log.
6. An awareness popup warns the user of how easily their data was recorded.

**VI. Sample Output**



**VII. How My Project Stands Out**

**1. True Global Keylogging**  
Unlike limited demos or form-based simulations, this project captures all keystrokes across any active window or app—mimicking how real malware behaves.

**2. Ethical Awareness-Focused Design**  
The purpose is not surveillance but education. The tool includes a visual log and a strong final message to alert the user of their vulnerability.

**3. Lightweight Yet Powerful**  
With minimal dependencies and code, it delivers a full simulation of a real-world threat, proving how low-effort attacks can have high impact.

**VIII. Challenges Faced**

* Preventing duplicate key entries or false triggers
* Avoiding interference with system performance during global key capture
* Designing a dark-themed, readable log viewer in Tkinter
* Ensuring the awareness popup is impactful without being alarming

**IX. Learning Outcomes**

* Gained experience using pynput for global event handling
* Learned how malware techniques can be repurposed for awareness
* Improved Python GUI skills for log visualization
* Understood the importance of creating **user-centric awareness tools** in cybersecurity

**X. Conclusion**

This project successfully replicates a real-world keylogger threat in a controlled and ethical environment. It teaches users how silently their data can be compromised, and encourages safer computing habits. The combination of hands-on demonstration and final awareness messaging makes it a strong educational cybersecurity tool.

**XI. References**

* [pynput Documentation – ReadTheDocs](https://pynput.readthedocs.io/)
* [Tkinter GUI – Python.org](https://docs.python.org/3/library/tkinter.html)
* OWASP Awareness GuidelineS
* KEYLOGGING ATTACKS- https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/keylogger/